InfoSec Research in Prominent IS Journals: Findings and Implications for the CIO and Board of Directors

Mark-David McLaughlin
Bentley University
Waltham, Massachusetts
mclaugh_mark@bentley.edu

Janis Gogan
Bentley University
Waltham, Massachusetts
jgogan@bentley.edu

Abstract

Having reviewed 91 information security (InfoSec) studies published in top IS journals for a ten-year period (2004-2014), we discuss technical, behavioral, financial, and managerial challenges for CIOs and boards of directors, and offer suggestions for future practice-relevant research on preventing, preparing for, detecting and responding to InfoSec incidents.

1. Introduction

The SIM 2015 IT Trends Study lists Security as the third highest IS investment priority (after Data Analytics and ERP) -- a sharp rise from #14 in 2013. Organizations daily confront InfoSec risks from malicious parties who steal data, intellectual property, and user credentials; harm software or data quality; and introduce malicious code that can cause systems to fail. Careless behavior by employees, customers, and partners also cause systems to fail or make it easier for attackers to compromise corporate systems and data. InfoSec incidents can damage an organization's reputation and financial health. Many attacks propagate both within and across organizations (via distributed denial of service attacks, exchange of malicious code in emails or social media, and other mechanisms). IT professionals, working under the direction of the CIO, try to *prevent* InfoSec incidents, *prepare* for events that will occur anyway (100% prevention is impossible), *detect* incidents that do occur, and rapidly and effectively *respond* to reduce negative impacts to organizations and their customers and business partners.

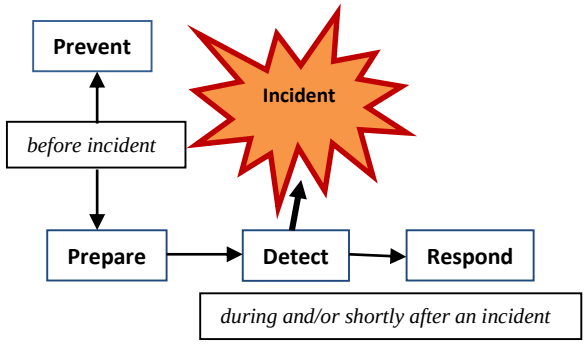

Figure 1: Phases of InfoSec Activities

Prior reviews [1] [2] find that behavioral, technical, organizational and other factors combine to affect Info-Sec preparation and compliance. A meta-review of 1280 papers notes that few relied on empirical research [3]. Another meta-review [4] reports that econometric models and attitude surveys prevail and that research with a stronger managerial focus is needed. Here, we discuss 91 empirical papers published over a ten year period (see Appendix 1) in the AIS Senior Scholars Basket of journals (EJIS, JAIS, JIT, JMIS, JSIS, ISJ, ISR, MISQ), including key findings and implications for the CIO and boards of directors. Our review method and justification are explained in the earlier meta-review [4].

Employees are a "weak link" in InfoSec [5], [6], and behavioral research seeks to understand why users fail to comply with InfoSec policies and guidelines. Despite efforts to test and strengthen General Deterrence Theory (GDT) and to combine it with theories of neutralization and organizational justice [7] [8] "weak-link" research reveals that organizations cannot expect employees, partners or customers to behave optimally. Humans are fallible; even with the best of intentions users take short cuts or fall prey to phishing and other social engineering attacks. Thus, both organizational InfoSec policies and practice-based research need to move beyond prevention, and focus at least as much on helping organizations effectively prepare for, detect and respond to the breaches that will inevitably occur.

The CIO answers to the board of directors on strategic IS governance issues, including InfoSec challenges. Boards are advised to annually review and critique their organization's IT security practices and disaster-recovery capabilities, and to stay abreast of best practices [9]. We examine these concerns through two lenses: topics (technical, behavioral, managerial) and security emphasis (prevent, prepare, detect, respond).

Author Note: Appendix 1 cites 91 papers comprising our review. To reference papers that were NOT part of the review set, we use numbered citations (HICSS format). To reference the 91 empirical papers in the review set, we use APA (Author, date) form. Also, in the sections that follow we provide a table listing the specific papers discussed in that section, in chronological order of publication.

URI: http://hdl.handle.net/10125/41819
ISBN: 978-0-9981331-0-2

2. InfoSec Risks and Impacts

Table 1 InfoSec Risks and Impacts Articles

Author/s	Journal	Year	Primary Aim
Cavusoglu et al.	ISR	2005	Detect
Cavusoglu et al.	JMIS	2008	Prevent
Cremonini and Nizovtsev	JMIS	2009	Prevent
Dey et al.	JMIS	2012	Prevent
Galbreth and Shor	MISQ	2010	Prevent
Goldstein et al.	JAIS	2011	Impacts
Gordon et al.	MISQ	2010	Impacts
Hua and Bapna	JSIS	2013	Prevent
Kumar et al.	JMIS	2008	Prevent
Mookerjee et al.	ISR	2011	Detect
Png and Wang	JMIS	2009	Prevent
Png et al	JMIS	2008	Prevent
Ransbotham and Mitra	ISR	2009	Detect
Wang et al.	ISR	2008	Prevent
Wang et al.	ISR	2013	Prevent
Yayla & Hu	JIT	2011	Impacts

With increases in attacks in recent years, boards need frequent updates from the CIO on incidents, standards, and challenges in their particular industries. In this section we review risk assessment studies that yield guidance for InfoSec investment decisions. These studies reveal that no one-size-fits-all rule answers the question of how much to spend on InfoSec, nor how to prioritize investments in specific tools or processes.

One research stream helps managers estimate the financial impacts of attacks. Rare high-cost incidents can distort managers' subsequent loss estimates, but combining daily loss (value-at-risk) data with extreme value analysis produces more accurate loss estimates (Wang et al. 2008). And, a test of a *resource weaknesses framework* [10] reveals that those InfoSec incidents that decrease IS resource availability (such as by shutting down a system or rendering data unavailable) cause greater financial losses than those which compromise data quality (Goldstein et al. 2011).

One theory suggests that disclosing investments in InfoSec tools/controls deters attackers (Cavusoglu et al. 2005). Penalties imposed by law enforcement also aim to deter future attackers (Cavusoglu et al. 2008), but this form of deterrence is *not* always effective, because well-informed attackers just shift their operations to countries with lower cybercrime conviction rates (Png *et al.* 2008). One paper suggests that higher-value firms (more attractive targets) should spend more to defend against malicious attacks, and enforcement agencies should focus on high-value targets (Png and Wang 2009).

Some attackers conduct reconnaissance before strategically choosing targets (Ransbotham and Mitra 2009), although one study finds that attackers derive little benefit from knowing whether a particular target has very strong or very weak protection (Mookerjee et al. 2011). A layered "defense-in-depth" security configuration contains controls that act as strategic substitutes, blocking attacks upstream (Kumar et al. 2008). Such layered controls might also deter attackers by signaling that an organization is committed to protecting its' IS resources (Cremonini and Nizovtsev 2010).

Do InfoSec-related disclosures influence companies' market value? InfoSec *investment* disclosures apparently *do* positively impact stock price (especially for e-commerce companies), but *incident* disclosures in annual reports do *not* (Gordon et al. 2010). One study based on the *efficient market hypothesis* also reports that InfoSec incident disclosures impact e-commerce firm stock prices more than brick-and-mortar firms, but increases in incident frequency lead to reduced market reaction intensity (Yayla and Hu, 2011). Also, disclosure of risk mitigation efforts is positively received by the market, and might lead to fewer subsequent security incidents (Wang et al. 2013). However, a firm that signals that it has invested in preventive InfoSec controls is not likely to deter a *cyber-terrorist* (Hua and Bapna 2013). A cyber-terrorist aims to destroy specific targets' IS resources for political reasons rather than personal gain. Some cyber-terrorists spend years researching targets, and generally they attack fewer organizations than cybercriminals.

What about InfoSec vulnerabilities in commercial software? This is a growing concern as organizations switch from custom software to off-the-shelf software products. When producers spend to develop new product features (for differentiation), they might spend loss on product security. Some attackers thus optimize their gains by targeting differentiated software products with large installed bases (Galbreth and Shor 2010). Generally, opportunistic and strategic attacker behavior influences security product effectiveness, ultimately affecting vendor prices (Dey et al. 2012).

3. Technical InfoSec Research

Table 2 Technical InfoSec Articles

Author/s	Journal	Year	Primary Aim
Abbasi et al.	MISQ	2010	Detect
Cavusoglu et al.	ISR	2009	Detect
D'Aubeterre et al.	JAIS	2008(a)	Prevent
D'Aubeterre et al.	EJIS	2008(b)	Prevent
Fernandez-Medina, et al.	EJIS	2007	Detect
Garfinkel et al.	ISR	2007	Prevent
Li & Sarkar	ISR	2006	Prevent
Li and Sarkar	ISR	2011	Prevent
Li and Sarkar	MISQ	2014	Prevent
Melville and McQuaid	ISR	2012	Prevent
Oetzel and Spiekermann	EJIS	2014	Prevent
Siponen et al.	JAIS	2006	Prevent
Wong et al.	ISJ	2012	Detect
Yue and Cakanyildirim	JMIS	2007	Detect

Designing and implementing the organization's InfoSec architecture is another important CIO concern. Each element must be assessed on its own and also in conjunction with each other element, to ensure that organizations neither over- nor under-invest in InfoSec capabilities and tools (Cavusoglu et al. 2009). Design science research investigates how to incorporate security elements into systems during development, or how to design specific tools for protecting hardware, software, and data. Each technique discussed next purports to prevent InfoSec breaches by incorporating protective features into systems or databases as they are designed. For example, a Systems Design Theory (Siponen et al. 2006) specifies six general requirements:

1. *Develop security features that resist … threats ….*
2. *Reflect customer's security requirements.*
3. *Provide abstract representation and operations for specifying three essential elements -- threats, objects and security features -- for three levels of abstraction – organizational, conceptual, technical.*
4. *Integrate SIS to normal ISD*
5. *Enable the autonomy of developers.*
6. *Adapt to forthcoming ISD methods.*

Security of a multidimensional data warehouse can be improved via a UML-based Access Control and Audit model (Fernandez-Medina et al. 2007), and information sharing can benefit from a Semantic Approach to Secure Collaborative Inter-Organizational eBusiness Processes (SSCIOBP; D'Aubeterre et al. 2008b) and Secure Activity Resource Coordination model (SARC; D'Aubeterre et al. 2008a). A systematic "privacy by design" problem representation structure supports analysis of shared-data privacy requirements (Oetzel and Spiekermann 2014).

Attackers use various techniques to reconstruct personally-identifiable information from redacted data sets. Addressing this problem, new ways to protect shared data have been proposed, such as random perturbation techniques for swapping data values (Li and Sarkar 2006; Li and Sarkar 2011; Melville and McQuaid 2012; Li and Sarkar 2014) and other statistical obfuscation techniques (Garfinkel et al. 2007).

Since 100% incident prevention is not possible, how can CIOs ensure that their organizations accurately, completely, and cost-effectively detect breaches early enough to limit harm from them? One paper, noting that intrusion detection system false alarms are expensive and disruptive, used a dynamic model to reveal "a trade-off between rapid reaction and high accuracy" (Yue and Cakanyildirim 2007 p. 350). To improve detection of fake web sites, organizations can also apply statistical learning theory (Abbasi et al. 2010) or develop an "artificial immune system" (Wong et al. 2012).

4. Behavioral InfoSec Research

Table 3 Behavioral InfoSec Articles

Author/s	Journal	Year	Primary Aim
Anderson and Agarwal	MISQ	2010	Prevent
Boss et al.	EJIS	2009	Prevent
Bulgurcu et al.	MISQ	2010	Prevent
Chen et al.	JMIS	2012	Prevent
D'Arcy et al.	ISR	2009	Prevent
D'Arcy, Herath, Shoss	JMIS	2014	Prevent
Dinev and Hu	JAIS	2007	Prevent
Dinev et al.	ISJ	2009	Prevent
Goel and Chengalur-Smith	JSIS	2010	Prevent
Guo et al.	JMIS	2011	Prevent
Hedstrom et al.	JSIS	2011	Prevent
Herath and Rao	EJIS	2009	Prevent
Herath et al.	ISJ	2014	Prevent
Hsu	EJIS	2009	Prevent
Johnston and Warkentin	MISQ	2010	Prevent
Karjalainen and Siponen	JAIS	2011	Prevent
Keith et al.	JAIS	2009	Prevent
Lee and Larsen	EJIS	2009	Prevent
Li et al.	ISJ	2014	Prevent
Liang and Xue	JAIS	2010	Prevent
Liang et al.	ISR	2014	Prevent
Myyry et al.	EJIS	2009	Prevent
Posey et al.	MISQ	2013	Prevent
Puhakainen and Siponen	MISQ	2010	Prevent
Siponen and Vance	MISQ	2010	Prevent
Tow et al.	JIT	2010	Prevent
Vaast	JSIS	2007	Holistic
Vance et al	JAIS	2014	Prevent
Vance et al.	JMIS	2013	Detect
Warkentin et al.	EJIS	2011	Prevent
Wright and Marett	JMIS	2010	Prevent
Wright et al.	ISR	2014	Prevent
Zhang et al.	EJIS	2009	Prevent

Many studies attempt to help organizations prevent breaches by improving user compliance with InfoSec policies (such as requiring use of strong passwords, restrictions on access to particular databases and software applications, and adherence to rules governing sharing of confidential data). A large body of work examined whether and to what extent users can be deterred from engaging in prohibited behaviors. Other studies challenged General Deterrence Theory (which proposes that penalty certainty, severity, and swiftness deters users from violating policies), and some studies enhanced GDT by incorporating factors addressed in other theories. Because GDT has received only weak or partial support, recent studies combined GDT with Protection Motivation Theory (PMT) [11], [12]. PMT proposes that two cognitive processes -- threat appraisal (threat severity, likelihood) and coping appraisal (efficacy of countermeasures and ability and cost to use them) -- influence individuals' attitudes about risks and risky behaviors. Studies demonstrate that *coping* appraisal influences employees' intentions to comply

with InfoSec rules, but that *threat* appraisal apparently does not improve user compliance -- perhaps because people underestimate risk likelihood and severity (Herath and Rao 2009). A PMT extension -- TTAT *(Technology Threat Avoidance Theory*) -- states that one first judges the likelihood of an attack, then judges one's ability to cope with it (Dinev and Hu 2007). TTAT predicted college students' use of anti-spyware software in a study that also concluded that avoidance and adoption are not polar opposites (Liang and Xue 2010). TTAT was subsequently integrated with the Technology Adoption Model (TAM) (Herath et al. 2014). A study that applied PMT to executive decision making found that IS expertise and industry IT focus influence executives' appraisal processes when making decisions about anti-malware software (Lee and Larsen 2009).

The *Theory of Planned Behavior* (TPB) [13] states that beliefs influence intentions, which influence behavior. Reserach that incorporated TPB reveals that users view *protective* security software (e.g., anti-virus software) differently than *productivity* software (such as spreadsheets). Self-efficacy and perceived ease of use, which influence acceptance and use of productivity software, does not significantly influence security software use. Policy "mandatoriness" also influences user compliance (Boss et al. 2009).

A *Theory of Accountability* [14] proposes that individuals feel pressure to justify their attitudes and behaviors to others. One study finds that audit logs influence user compliance with InfoSec rules, through four influential aspects: identifiability, user awareness of logging and of audits, and electronic presence (Vance et al. 2013). Rewards also influence compliance attitudes (Bulgurcu et al. 2010; Liang et al. 2014), and research also suggests that users are more receptive to messages emphasizing positive outcomes of compliance (Anderson and Agarwal 2010), rather than negative outcomes of non-compliance (fear appeals). However, (which proposes that penalty certainty, severity, and swiftness deters users from violating policies) combining social influence and self-efficacy with a message that consequences of non-compliance will be severe did predict user compliance in one study (Johnston and Warkentin 2010). Building on these prior studies, a *Composite Behavior Model* (Guo et al. 2011) proposes that users' InfoSec compliance intentions are influenced by attitudes, habit, expected rewards or punishments, identity, and others' disapproval or approval of specific behavior. Alternatively, a *Theory of Protection-Motivated Behavior Diversity* (Posey et al. 2013) proposes that individuals judge protective behaviors along three main dimensions: difficulty, degree of criticality, and common sense.

Experiments have yielded particularly intriguing findings. One experiment compared rewards (positive control) versus deterrence (non-compliance penalties), revealing a strong relationship between rewards and compliance and a strong interaction effect between reward and punishment (Chen et al. 2012). Another experiment (Vance et al. 2014) measured electrical activity (EEG) in sections of subjects' brains associated with risk-taking. Before a simulated incident, subjects' surveyed behavior intentions did not correlate with EEG readings. After the incident, subjects' threat assessment survey answers did correlate with EEG readings. Another experiment studied why some users fall victim to security attacks such as phishing. Computer self-efficacy, prior experience with computer attacks, security awareness, and general suspicion of humanity were significantly associated with subjects' ability to resist "phishy" e-mails, while perceived risk of attack was not (Wright and Marett 2010). Another experiment showed that the following attacker influence techniques increase users' vulnerability to phishing: "liking," social proof, scarcity, reciprocity (Wright et al. 2014).

Why don't employees just do the "right" thing (comply with safe computing rules)? A study of anti-spyware usage in the US versus South Korea (Dinev et al. 2009) suggests that national culture influences compliance, and regardless of national culture, employees are also influenced by social norms. In some contexts, non-compliance with security rules is seen as morally acceptable; in such contexts perceived certainty of getting caught influences user compliance. In contexts where violations are seen as reprehensible, penalty severity has a stronger effect (D'Arcy et al. 2009). Users are more likely to engage in risky behaviors when expected benefits are high (Tow et al. 2010). A study that combined theories of *Moral Development* [15] and *Motivational Types of Values* [16] reports no significant relationship between users' moral values and their attitudes toward InfoSec practices (Myyry et al. 2009). Another study (D'Arcy et al. 2014) combined *Coping Theory* [17] and *Moral Disengagement Theory* [18] to propose that conflict between individuals' values and organizations' policies leads employees to rationalize their policy violations. Studies testing *Neutralization Theory* [19] find that wrongdoers rationalize ("neutralize") their bad behavior via five techniques: denial of responsibility, denial of injury, denial of the victim, condemnation of condemners, appeal to higher loyalties. A large-scale survey found no relationship between penalties and compliance intentions (thus, did not support GDT), but strong support for Neutralization Theory in explaining non-compliance intentions (Siponen and Vance 2010). Lastly, employees' beliefs about procedural, interpersonal, informational, and distributive *justice* [20] may more strongly influence InfoSec compliance

intention than certainty or severity of non-compliance penalties (Li et al. 2014).

Other behavioral studies analyzed how users interact with specific InfoSec tools. For example, although strong passwords help prevent unauthorized system access, many people avoid using them due to difficulty recalling multiple passwords for different systems with varied password complexity rules (Zhang et al. 2009). A study reveals that well-chosen passphrases, based on longer sentences are easier for users to remember and use (Keith et al. 2009). Hypothesizing that the clarity of a written InfoSec policy affects user comprehension (in turn influencing whether and to what extent the policy is effective) Goel and Chengalur-Smith (2010) asked 68 graduate students to rate InfoSec policies per 22 rhetorical clarity measures. Other studies reveal that InfoSec awareness training is more effective when it is seen as personally relevant, taps into learners' systematic cognitive information processing, and takes into account each learner's existing knowledge (Puhakainen and Siponen 2010). Top management support influences employee compliance, and informal knowledge distribution (per S*ocial Learning Theory* and distinct from formal training methods) influences employee perceived self-efficacy, ultimately increasing InfoSec policy compliance (Warkentin et al. 2011). See also Karjalainen and Siponen (2011).

Exploratory case studies directly examined users' attitudes and behaviors. Vaast (2007) observes that specific work practices affect InfoSec programs, and that a security awareness initiative is more effective when customized for each work group. A longitudinal case study of two hospitals (Hedström et al. 2011) demonstrated further support for Vaast's *Social Representations* [21] perspective, and challenged GDT by arguing that organizations should link user values to InfoSec rules, rather than relying on strict rules and penalties. Another case study used *Frames Analysis* (assumptions, interpretations, expectations, knowledge) to reveal that specific work practices, routines, and InfoSec attitudes at a Taiwanese firm influenced employees' awareness and compliance (Hsu 2009).

To summarize behavioral InfoSec research from the perspective of the CIO and Board of Directors: we cannot reliably deter problematic behavior. Some papers conclude that deterrence is not effective and/or that rewards and context-specific training are more powerful than penalties. Educational campaigns that change employees' understanding, attitudes, and work practices might reduce InfoSec violations and help prevent breaches or mistakes – if training is aligned with workgroup practices, formal and informal norms, and individuals' prior knowledge. More behavioral research is needed to yield clear results that can guide management practice, but to date the best managerial advice emerging from this InfoSec stream is: reward good behavior, penalize rule violations, offer training that helps each user recognize how his/her behavior can weaken or strengthen the information security chain. Above all, do not rely on fallible human users.

In our set of 40 behavioral studies, most aimed to help organizations prevent InfoSec breaches by inducing employees to adhere to required practices. While prevention is certainly an important aim, it is not enough. The CIO and board would benefit from studies that reveal how employees actually do prepare for the InfoSec incidents that will inevitably occur (such as by participating in contingency planning and "fire drills"), and to what extent employees make use of tools and information sources that detect suspicious behavior or potentially damaging breaches. Leaders also need to know how employees actually respond when incidents occur. For example, to what extent do they refer to and follow the contingency plan? To what extent do they improvise their responses? What specific employee behaviors contribute to effective and rapid response that minimizes harm to customers, other partners, fellow employees, and valuable financial, IT, and data assets? Conversely, what specific employee behaviors impede effective InfoSec incident response?

We also note that many papers (23 of 40 behavioral studies in our review set) relied on attitude surveys and did not observe or directly measure user behavior. Given that employees are a weak link in the information security chain, it is problematic that just three behavioral studies were based on case research exploring employee attitudes and behavior in specific work contexts. Well-designed case studies contribute important findings by revealing how social context and work practices interact with employee attitudes, intentions, and behavior.

5. Managerial InfoSec Research

Table 4 (below) summarizes the managerial InfoSec papers in our review set. Some studies directly focused on security policies and practices that managers set and oversee, and some studies considered the InfoSec implications of new end-user technologies. For example, a study guided by *Control Theory* [22] concludes that new wireless network security mechanisms should be coupled with workflow changes and policies for acceptable wireless systems use (Katos and Adams, 2005). An action research study in a multinational firm used a Bayesian evidential reasoning approach to perform a cost-benefit risk analysis that accounted for uncertainty (Sun et al. 2006). An intriguing content analysis of 400,000+ searches in file sharing networks (Johnson 2008) demonstrates that mobile device use increases the risk that a firm's confidential data will be compromised. At greatest risk:

large, highly visible firms with many retail accounts, and firms that experienced prior data losses. Analysis of an organization's e-mail and spam data validated a Bayesian real options model (Herath and Herath 2008), and another risk assessment method combined five financial metrics (labor cost, lost profit, information asset value, business process cost, stock price) with qualitative risks (systems, systems security, information, business, shareholders) (Salmela 2008).

Table 4 Managerial InfoSec Articles

Author/s	Journal	Year	Primary Aim
Arora et al.	ISR	2010	Prevent
August and Tunca	ISR	2008	Prevent
August et al.	ISR	2014	Prevent
Backhouse et al.	MISQ	2006	Prevent
Chen, et al.	MISQ	2011	Prevent
Culnan and Williams	MISQ	2009	Prevent
Dhillon and Torkzsedeh	ISJ	2006	Holistic
Gal-Or & Ghose	ISR	2005	Prepare
Gupta and Zhdanov	MISQ	2012	Prevent
Herath and Herath	JMIS	2008	Prevent
Hsu et al.	ISR	2012	Prevent
Hu et al.	JSIS	2007	Prevent
Hui et al.	JMIS	2013	Prevent
Johnson	JMIS	2008	Prevent
Katos and Adams	JSIS	2005	Prevent
Kim and Kim	MISQ	2014	Prevent
Kwon and Johnson	JMIS	2013	Prevent
Kwon and Johnson	MISQ	2014	Prevent
Lee et al.	ISR	2013	Prevent
Njenga and Brown	EJIS	2012	Respond
Ransbotham et al.	MISQ	2012	Detect
Salmela	JIT	2008	Impacts
Smith et al.	MISQ	2010	Prevent
Spears and Barki	MISQ	2010	Prevent
Stahl et al.	ISJ	2012	Prevent
Sun et al.	JMIS	2006	Impacts
Temizkan et al.	JMIS	2012	Prevent
Zhao et al.	JMIS	2013	Impacts

Other research yields guidance for managerial oversight of information security. A study based on more than 100 interviews (Dhillon and Torkzadeh 2006) identified nine "value-focused" objectives essential for managing information security:

1. *Enhance management development practices.*
2. *Strengthen human resource management practices.*
3. *Develop and sustain an ethical environment.*
4. *Maximize access controls.*
5. *Promote individual work ethic.*
6. *Maximize data integrity.*
7. *Enhance integrity of business processes.*
8. *Maximize privacy.*
9. *Maximize organizational integrity*.

Analysis of a national software vulnerability database suggests that adoption of diverse software configurations/versions reduces risk across a network of organizations, whereas (ironically) adoption of security standards or best practices increases risk. This is because a standard configuration will share common vulnerabilities, leading to "correlated failures," in which attackers identify a weakness in one organization's standard implementation and exploit it in others, compromising an entire network (Chen et al. 2011).

Focusing on privacy implications of information security, breaches at TJX and Choicepoint were compared through the lens of *Normative Ethics*, and leaders are advised to focus on three objectives: create a culture of privacy, ensure accountability, avoid decoupling of InfoSec practices and policies (Culnan and Williams 2009). Emphasizing employees as partners rather than "weak link," another study, guided by a *Buy-in Theory of Participation* [23] and *Emergent Interactions Theory* [24], concludes that InfoSec controls are more effective when users help to prioritize, analyze, design, implement, test, and monitor them (Spears and Barki 2010).

Institutional Theory [25] was tested in a study of how and why one large company adopted various security policies, practices, and technologies (Hu et al. 2007; Hsu et al. 2012). Coercion (laws and regulations) and norms (social influence by opinion leaders) were influential, but imitation (of other firms' policies, practices or technology choices) was not. Senior management support and employee awareness reportedly contribute to successful InfoSec management.

A case study at the UK National Health Service (Stahl et al. 2012) finds that senior management support and ideology influenced the creation of security policies. However, vague InfoSec policies and those based on unfamiliar language left the Health Service open to varied interpretations, which limited their effectiveness in guiding or controlling behavior. Another case study, of five large multinational companies in South Africa, finds that during early response to an InfoSec incident, improvisation improved effectiveness -- presumably by bridging "unavoidable gaps between formal standards/procedures and emergent events" (Njenga and Brown 2012).

Does security compliance maturity matter? Archival data from 250 health care organizations reveals that in those with mature certified security programs, managers express interest in protecting data, and tend to view breaches as evidence of security program failure (Kwon and Johnson 2013). A survey (Kwon and Johnson 2014) finds that investments in prevention significantly reduce data breaches, and that organizational learning mediates InfoSec investment and security performance, especially in the presence of external pressures.

Combining the theories of *Threat Disclosure Benefits* and *Resource Complements*, a study of inter-

organizational information sharing (Gal-Or and Ghose 2005) proposes that large organizations in highly competitive industries have strong incentives to share information about InfoSec vulnerabilities, threats, and attacks. A test of *Learning Theory* (Kim and Kim 2014) finds that prior software development experience helps a software firm produce anti-virus products that are able to rapidly detect malware. Prior experience with many software products helps developers produce malware detection products for the general public, but within-family experience is more effective for developing products for detecting targeted attacks.

Large vendors and open source vendors reportedly release security patches faster than smaller vendors, patches are released more quickly for vulnerabilities that represent higher threat severity, and public disclosure by third parties causes vendors to release patches more quickly (Arora 2010). Analysis of patch release behavior through the well-known information quality categories of *confidentiality, integrity*, and *availability* [26] reveals that patches addressing confidentiality or integrity risks are released faster than patches addressing availability risks (Temizkan et al. 2012).

Legislative pressure might lead vendors to release patches more quickly, and release timing also depends on whether a vendor has a policy of distributing fixes only in new software releases or is in the habit of releasing frequent updates. Also, compared with open disclosure, vulnerabilities disclosed through a market mechanism reportedly take longer to be exploited and are exploited less often (Ransbotham et al. 2012*)*. Pirated software is a special case; should legitimate producers give patches to illegitimate users? One study demonstrated that software vendors receive higher profits when they provide security patches to users of illegally obtained software (August and Tunca 2008).

Use of a managed security service provider (MSSP) can give rise to "system interdependency risks" (Hui et al. 2012). This can happen if the MSSP configures its software to conform to standards and best practices (leading to correlated failure risk, which increases along with growth of the customer base). Use of an MSSP may also give rise to a *double moral hazard* (lack of caution when risk is transferred to another organization), particularly if the MSSP is not transparent about its security practices or is averse to investing in security measures not deemed absolutely necessary to protect their clients. A proposed optimal solution is for the MSSP to offer multilateral contracts, specifying that if any one client experiences a security incident, the MSSP will compensate all clients (Lee it al. 2013). Cyber-insurance might be a better way to reduce risk than transferring risk to an MSSP or entering into a risk pooling arrange-ment (Zhao et al. 2013). Each option offers different exposure and security investment efficiency. A *proportional hazard model* demonstrates that vendors that provide both on-premises and cloud-based services invest more in on-premises security than security providers based only in the cloud (August et al. 2014).

Information security standards are developed through inter-organizational collaboration. A case study about BS7799 -- the first security standard proposed by the UK Department of Trade and Industry (DTI) -- extended the *circuits of power* framework [27] to examine human, economic, and social factors influencing this standard's development (Backhouse et al. 2006). Because consensus was required, the standard was heavily influenced by organizations with extensive political capital -- more so than by economic or strategic incentives. A New South Wales agencies' mandatory adoption of ISO InfoSec standard 27001:2006 (Smith et al. 2010) was reportedly influenced by the perceived legitimacy of the central government and compatibility of the standard with existing work practices. Limited resources, low senior management involvement, group norms, and cultural biases inhibited adoption. In general, research indicates that effective inter-organizational information-sharing and collaboration help improve information security. However network traffic data from an ACM Special Interest Group reveals that joining a non-profit consortium is impractical for many organizations, due to high start-up costs, inability to reach economies of scale, transparency issues, and other factors (Gupta and Zhdanov 2012).

Managerially-focused InfoSec research has yielded useful findings for the CIO and boards of directors. New techniques for estimating InfoSec risks can help the CIO justify investments in protective tools and resources (and the CIO needs to continually re-evaluate the organization's level of protection). Managerially-focused studies also reveal how varied contexts (within or beyond organizational boundaries) influence InfoSec policies and their effectiveness. Unfortunately, no silver bullet protects organizations. The CIO needs to ensure that complementary tools, policies, procedures, and human, financial, and technical resources are in place; that every element is effective; and that the organization has neither under- nor over-invested in redundant InfoSec protection. The board needs to ensure that other C-level executives understand how correlated security failures arise and why inter-organizational collaboration is needed, as well as the vital importance of employee training, participation, and vigilance. A team effort is needed to achieve and sustain a system of effective internal controls and rewards and to instill a culture of accountability and shared respect for the confidentiality, integrity and controlled availability of IS resources.

6. Discussion

Boards of directors need to work closely with the CIO to ensure the security of organizational systems and data. They can start by asking two key questions (similar to those suggested by Nolan and McFarlan [9]):

- *How strong is our InfoSec prevention*?
- *Are we prepared for incidents that will surely occur, and do our employees and partners know what to do when an InfoSec incident does occur?*

Most papers in our ten-year review set, (71 of 91 papers) focused on preventing InfoSec incidents by establishing policies, incentives, and sanctions to induce employees to comply with safe computing practices. However, InfoSec incidents continue to occur on a daily basis (including breaches that compromise personally identifiable information and threaten organizations' reputation and financial standing). Thus, preventive InfoSec controls cannot as yet be considered reliable. Therefore, more research is needed that examines (and produces findings that ultimately improve) InfoSec incident preparation, detection and response. Ten studies in our review set examined technical, human, and/or economic InfoSec incident detection challenges. Two studies took a helpful managerial approach which we label "holistic". Just one study (Njenga and Brown 2012) actually examined incident response.

Thus, two broad topics have been understudied by IS researchers (at least, in the AIS Senior Scholars Basket):

- InfoSec Incident Preparation (recognize InfoSec incidents will likely occur despite preventive controls; establish an incident response team and put a viable incident response plan in place; educate employees on their roles during and immediately following incidents; rehearse responses)
- InfoSec Incident Response (ensure that employees and business partners adhere to the incident response plan and improvise appropriately)

These topics are of great concern to boards of directors, particularly given risks – such as lost market value, lost customer trust, and embarrassment – that accompany large-scale breaches. Certainly the Target breach, and other recent high-profile incidents that led CIOs to lose their jobs, are important cautionary tales. Business-research partnerships that foster more studies on preparation and response are greatly needed.

Practitioners are also invited to approve or sponsor case studies and other interactive forms of InfoSec research. Considering the 91 papers in our review set in light of research methods used (Appendix 1), we see that although many attitude surveys were conducted and many econometric models were built, only eight case studies were conducted. Longitudinal case studies can help reveal how employee or business partner InfoSec compliance or non-compliance changes over time, and can also continue to explore how varied cultural and work contexts affect organizations' vulnerability to breaches. Comparative case studies might reveal how various combinations of penalties, rewards, and education play out in organizations of varying sizes in various industries, populated by employees with different educational and skill levels, and other dimensions. More importantly, given the topical imbalance just observed, new case studies need to closely examine whether and how organizations prepare for and respond to InfoSec incidents, and to what extent members of formal incident response teams, and others in and beyond the organization, work effectively to protect resources and preserve valuable relationships with customers and business partners. This under-studied subject is in need of immediate attention.

A handful of action research InfoSec studies were published in our review set, along with 12 design science studies. Interactive research methods such as these help to ensure that studies are relevant and produce useful tools that IS organizations, employees, and managers can put to use. Perhaps it is time for a new group of interactive researchers to focus on incident preparation and response, which are not yet represented in this set of action research and design science studies.

We conclude that, while existing behavioral, economic and technical scholars may prefer to continue on the research journeys they have already embarked upon, there is ample space for qualitative scholars (especially case researchers) and interactive scholars (those who excel at action research or design science) to investigate InfoSec incident preparation and response, and to offer valuable findings that the CIO and the Board of Directors can put to good use. Thus, research arising from new researcher-industry partnerships (which are often sponsored by CIOs and/or executive-level industry leaders) might benefit greatly from a focus on InfoSec incident preparation and response, using case studies or interactive research methods.

7. References

[1] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspect-ives," *Inf. Syst. J.*, vol. 11, no. 2, pp. 127–153, Apr. 2001.

[2] M. T. Siponen, "An analysis of the traditional IS security approaches: implications for research and practice," *Eur. J. Inf. Syst.*, vol. 14, no. 3, pp. 303–315, Sep. 2005.

[3] M. Siponen, R. Willison, and R. Baskerville, "Power and practice in information systems security research," in *ICIS 2008 Proceedings*, 2008, p. 26.

[4] M.-D. McLaughlin and J. Gogan, "INFOSEC in a Basket, 2004-2013," in *AMCIS*, Savannah, GA, 2014.

[5] C. Posey, T. L. Roberts, P. B. Lowry, R. J. Bennett, and J. F. Courtney, "Insiders' Protection of Organizational Information Assets: Development," *Mis Q.*, vol. 37, no. 4, p. 1189–+, Dec. 2013.
[6] I. Arce, "The weakest link revisited [information security]," *Secur. Priv. IEEE*, vol. 1, no. 2, pp. 72–76, 2003.
[7] J. D'Arcy and T. Herath, "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings," *Eur. J. Inf. Syst.*, vol. 20, no. 6, pp. 643–658, Nov. 2011.
[8] R. Willison and M. Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Q.*, vol. 37, no. 1, pp. 1–20, Mar. 2013.
[9] R. Nolan and F. W. McFarlan, "Information technology and the board of directors," *Harv. Bus. Rev.*, vol. 83, no. 10, p. 96, 2005.
[10] B. Wernerfelt, "A resource-based view of the firm," *Strateg. Manag. J.*, vol. 5, no. 2, pp. 171–180, 1984.
[11] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975.
[12] R. W. Rogers, J. T. Cacioppo, and R. Petty, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social psychophysiology: A sourcebook*, 1983, pp. 153–177.
[13] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1991.
[14] P. E. Tetlock, "Accountability and complexity of thought.," *J. Pers. Soc. Psychol.*, vol. 45, no. 1, p. 74, 1983.
[15] L. Kohlberg, *Stage and sequence: The cognitive-developmental approach to socialization*. Chicago, IL: Rand McNally, 1969.
[16] S. H. Schwartz, "Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries," *Adv. Exp. Soc. Psychol.*, vol. 25, no. 1, pp. 1–65, 1992.
[17] R. S. Lazarus and S. Folkman, "Stress, Appraisal, and Coping," *N. Y. Springer*, 1984.
[18] A. Bandura, "Social cognitive theory of moral thought and action," *Handb. Moral Behav. Dev.*, vol. 1, pp. 45–103, 1991.
[19] G. M. Sykes and D. Matza, "Techniques of neutralization: A theory of delinquency," *Am. Sociol. Rev.*, vol. 22, no. 6, pp. 664–670, 1957.
[20] J. S. Adams, "Inequity in social exchange," *Adv. Exp. Soc. Psychol.*, vol. 2, no. 267–299, 1965.
[21] S. Moscovici, *La psychanalyse, son image et son public: étude sur la représentation sociale de la psychanalyse*. Presses Universitaires de France, 1961.
[22] A. Hawker, *Security and control in information systems: A guide for business and accounting*, vol. 1. Psychology Press, 2000.
[23] H. Barki and J. Hartwick, "Rethinking the concept of user involvement," *MIS Q.*, pp. 53–63, 1989.
[24] M. L. Markus and J.-Y. Mao, "Participation in development and implementation-updating an old, tired concept for today's IS contexts," *J. Assoc. Inf. Syst.*, vol. 5, no. 11, p. 14, 2004.
[25] P. DiMaggio and W. W. Powell, *The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields*. Chicago, IL: University of Chicago Press, 1991.
[26] D. B. Parker, *Fighting computer crime: A New Framework for Protecting Information*. John Wiley & Sons, Inc. New York, NY, 1998.
[27] S. R. Clegg, *Frameworks of power*. Sage, 1989.

APPENDIX 1 InfoSec Studies in the Basket: Partial Citations and Description

Author/s	Journal	Year	Method	Primary Perspective	Primary Aim
Abbasi et al.	MISQ	2010	DS+MOD+EXP	Technical	Detect
Anderson and Agarwal	MISQ	2010	SURV+EXP	Behavioral	Prevent
Arora et al.	ISR	2010	QUANT	Managerial	Prevent
August and Tunca	ISR	2008	MOD	Managerial	Prevent
August et al.	ISR	2014	MOD	Managerial	Prevent
Backhouse et al.	MISQ	2006	CASE	Managerial	Prevent
Boss et al.	EJIS	2009	SURV	Behavioral	Prevent
Bulgurcu et al.	MISQ	2010	SURV	Behavioral	Prevent
Cavusoglu et al.	ISR	2005	MOD	Technical	Detect
Cavusoglu et al.	JMIS	2008	MOD	Technical	Prevent
Cavusoglu et al.	ISR	2009	DS+MOD	Technical	Detect
Chen et al.	JMIS	2012	EXP	Behavioral	Prevent
Chen, et al.	MISQ	2011	MOD	Managerial	Prevent
Cremonini and Nizovtsev	JMIS	2009	MOD	Managerial	Prevent
Culnan and Williams	MISQ	2009	CASE	Managerial	Prevent
D'Arcy et al.	ISR	2009	SURV	Behavioral	Prevent
D'Arcy, Herath, Shoss	JMIS	2014	SURV	Behavioral	Prevent
D'Aubeterre et al.	EJIS	2008(b)	DS+MOD	Technical	Prevent
D'Aubeterre et al.	JAIS	2008(a)	DS+MOD	Technical	Prevent
Dey et al.	JMIS	2012	MOD	Economic	Prevent
Dhillon and Torkzsedeh	ISJ	2006	QUAL	Managerial	Holistic
Dinev and Hu	JAIS	2007	SURV	Behavioral	Prevent
Dinev et al.	ISJ	2009	SURV	Behavioral	Prevent
Fernandez-Medina, et al.	EJIS	2007	DS	Technical	Detect
Galbreth and Shor	MISQ	2010	MOD	Managerial	Prevent
Gal-Or & Ghose	ISR	2005	MOD	Managerial	Prepare
Garfinkel et al.	ISR	2007	DS+MOD	Technical	Prevent
Goel and Chengalur-Smith	JSIS	2010	SURV+QUAL	Managerial	Prevent
Goldstein et al.	JAIS	2011	QUANT	Managerial	Impacts
Gordon et al.	MISQ	2010	QUANT	Managerial	Impacts
Guo et al.	JMIS	2011	SURV	Behavioral	Prevent

Gupta and Zhdanov	MISQ	2012	MOD	Managerial	Prevent
Hedstrom et al.	JSIS	2011	CASE	Behavioral	Prevent
Herath and Herath	JMIS	2008	MOD	Managerial	Prevent
Herath and Rao	EJIS	2009	SURV	Behavioral	Prevent
Herath et al.	ISJ	2014	SURV	Behavioral	Prevent
Hsu	EJIS	2009	CASE	Managerial	Prevent
Hsu et al.	ISR	2012	QUAL+SURV	Managerial	Prevent
Hu et al.	JSIS	2007	CASE	Managerial	Prevent
Hua and Bapna	JSIS	2013	MOD	Managerial	Prevent
Hui et al.	JMIS	2013	MOD	Managerial	Prevent
Johnson	JMIS	2008	QUANT	Managerial	Prevent
Johnston and Warkentin	MISQ	2010	SURV+EXP	Behavioral	Prevent
Karjalainen and Siponen	JAIS	2011	SURV	Managerial	Prevent
Katos and Adams	JSIS	2005	MOD	Managerial	Prevent
Keith et al.	JAIS	2009	EXP	Behavioral	Prevent
Kim and Kim	MISQ	2014	MOD	Managerial	Prevent
Kumar et al.	JMIS	2008	MOD	Risk & Impacts	Prevent
Kwon and Johnson	JMIS	2013	SURV	Managerial	Prevent
Kwon and Johnson	MISQ	2014	MOD	Managerial	Prevent
Lee and Larsen	EJIS	2009	SURV	Behavioral	Prevent
Lee et al.	ISR	2013	MOD	Managerial	Prevent
Li & Sarkar	ISR	2006	DS+MOD	Technical	Prevent
Li and Sarkar	ISR	2011	DS+MOD	Technical	Prevent
Li and Sarkar	MISQ	2014	DS+MOD	Technical	Prevent
Li et al.	ISJ	2014	SURV	Behavioral	Prevent
Liang and Xue	JAIS	2010	SURV	Behavioral	Prevent
Liang et al.	ISR	2014	SURV	Behavioral	Prevent
Melville and McQuaid	ISR	2012	DS+MOD	Technical	Prevent
Mookerjee et al.	ISR	2011	MOD	Managerial	Detect
Myyry et al.	EJIS	2009	SURV	Behavioral	Prevent
Njenga and Brown	EJIS	2012	CASE	Managerial	Respond
Oetzel and Spiekermann	EJIS	2014	MOD	Technical	Prevent
Png and Wang	JMIS	2009	MOD	Economic	Prevent
Png et al	JMIS	2008	MOD	Economic	Prevent
Posey et al.	MISQ	2013	QUAL+ SURV	Behavioral	Prevent
Puhakainen and Siponen	MISQ	2010	AR+SURV	Behavioral	Prevent
Ransbotham and Mitra	ISR	2009	QUAL+QUANT	Managerial	Detect
Ransbotham et al.	MISQ	2012	QUANT	Economic	Detect
Salmela	JIT	2008	AR	Managerial	Impacts
Siponen and Vance	MISQ	2010	SURV	Behavioral	Prevent
Siponen et al.	JAIS	2006	DS+AR	Technical	Prevent
Smith et al.	MISQ	2010	AR+SURV	Managerial	Prevent
Spears and Barki	MISQ	2010	QUAL+SURV	Managerial	Prevent
Stahl et al.	ISJ	2012	CASE	Managerial	Prevent
Sun et al.	JMIS	2006	AR	Managerial	Impacts
Temizkan et al.	JMIS	2012	QUANT	Managerial	Prevent
Tow et al.	JIT	2010	QUAL+SURV	Behavioral	Prevent
Vaast	JSIS	2007	CASE	Managerial	Holistic
Vance et al	JAIS	2014	SURV+EXP	Behavioral	Prevent
Vance et al.	JMIS	2013	SURV	Behavioral	Detect
Wang et al.	ISR	2008	QUAL+MOD	Managerial	Prevent
Wang et al.	ISR	2013	EXP+QUAL	Managerial	Prevent
Warkentin et al.	EJIS	2011	SURV	Behavioral	Prevent
Wong et al.	ISJ	2012	DS+MOD+EXP	Technical	Detect
Wright and Marett	JMIS	2010	EXP	Behavioral	Prevent
Wright et al.	ISR	2014	EXP	Behavioral	Prevent
Yayla & Hu	JIT	2011	QUANT	Managerial	Impacts
Yue and Cakanyildirim	JMIS	2007	MOD	Technical	Detect
Zhang et al.	EJIS	2009	EXP	Behavioral	Prevent
Zhao et al.	JMIS	2013	MOD	Managerial	Impacts